

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-278

Vulnerability Summary for the Week of September 28, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
alibabaclone -- alibaba_clone	SQL injection vulnerability in offers_buy.php in Alibaba Clone 3.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-09-30	7.5	CVE-2009-3504 VUPEN SECUNIA MISC	
apple -- safari	Apple Safari, possibly before 4.0.3, on Mac OS X does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-29	7.5	CVE-2009-3455 BID	
avast -- avast_antivirus_home avast -- avast_antivirus_professional	Stack-based buffer overflow in aswMon2.sys in avast! Home and Professional for Windows 4.8.1351, and possibly other versions before 4.8.1356, allows local users to cause a denial of service (system crash) and possibly gain privileges via a crafted IOCTL request to IOCTL oxb2c80018.	2009-10-01	7.2	CVE-2009-3522 MISC XF VUPEN SECTRACK BID BUGTRAQ CONFIRM SECUNIA OSVDB	

avast -- avast_antivirus_home avast -- avast_antivirus_professional	Unspecified vulnerability in ashWsFtr.dll in avast! Home and Professional for Windows before 4.8.1356 has unknown impact and local attack vectors.	2009-10-01	7.2	CVE-2009-3524 CONFIRM SECUNIA OSVDB
bpowerhouse -- bplawyercasedocuments	SQL injection vulnerability in employee.aspx in BPowHouse BPLawyerCaseDocuments 1.0 allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-09-30	7.5	CVE-2009-3499 VUPEN SECUNIA MISC
bpowerhouse -- bpgames	Multiple SQL injection vulnerabilities in BPowHouse BPGames 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) cat_id parameter to main.php and (2) game_id parameter to game.php.	2009-09-30	7.5	CVE-2009-3500 VUPEN SECUNIA MISC
bpowerhouse -- bpstudents	SQL injection vulnerability in students.php in BPowHouse BPStudents 1.0 allows remote attackers to execute arbitrary SQL commands via the test parameter in a preview action.	2009-09-30	7.5	CVE-2009-3501 XF VUPEN SECUNIA MISC OSVDB
bpowerhouse -- bpmusic	SQL injection vulnerability in music.php in BPowHouse BPMusic 1.0 allows remote attackers to execute arbitrary SQL commands via the music_id parameter.	2009-09-30	7.5	CVE-2009-3502 VUPEN SECUNIA MISC
bpowerhouse -- bpholidaylettings	Multiple SQL injection vulnerabilities in search.aspx in BPowHouse BPHolidayLettings 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) rid and (2) tid parameters.	2009-09-30	7.5	CVE-2009-3503 VUPEN SECUNIA MISC
cisco -- ios	Race condition in the Firewall Authentication Proxy feature in Cisco IOS 12.0 through 12.4 allows remote attackers to bypass authentication, or bypass the consent web page, via a crafted request, aka Bug ID CSCsy15227.	2009-09-28	7.1	CVE-2009-2863 XF SECTRACK BID CISCO CONFIRM OSVDB
cisco -- unified_callmanager cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 5.x before 5.1(3g), 6.x before 6.1(4), 7.0.x before 7.0(2a)su1, and 7.1.x before 7.1(2) allows remote attackers to cause a denial of service (service restart) via malformed SIP messages, aka Bug ID CSCsz95423.	2009-09-28	7.8	CVE-2009-2864 CONFIRM
cisco -- unified_communications_manager_express cisco -- ios	Buffer overflow in the login implementation in the Extension Mobility feature in the Unified Communications Manager Express (CME) component in Cisco IOS 12.4XW, 12.4XY, 12.4XZ, and 12.4YA allows remote attackers to execute arbitrary code or cause a denial of service via crafted HTTP requests, aka Bug ID CSCsq58779.	2009-09-28	7.6	CVE-2009-2865 CISCO CONFIRM
	Unspecified vulnerability in Cisco IOS 12.2 through 12.4 allows remote attackers to cause	2009-09-28		CVE-2009-2866

cisco -- ios	a denial of service (device reload) via a crafted H.323 packet, aka Bug ID CSCsz38104.	2009-09-28	7.8	2009 CISCO CONFIRM
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.2XNA, 12.2XNB, 12.2XNC, 12.2XND, 12.4T, 12.4XZ, and 12.4YA, when Zone-Based Policy Firewall SIP Inspection is enabled, allows remote attackers to cause a denial of service (device reload) via a crafted SIP transit packet, aka Bug ID CSCsr18691.	2009-09-28	7.8	CVE-2009-2867 VUPEN SECTRACK CISCO CONFIRM
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.2 through 12.4, when certificate-based authentication is enabled for IKE, allows remote attackers to cause a denial of service (Phase 1 SA exhaustion) via crafted requests, aka Bug IDs CSCsy07555 and CSCee72997.	2009-09-28	7.8	CVE-2009-2868 VUPEN CISCO CONFIRM
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.2XNA, 12.2XNB, 12.2XNC, 12.2XND, 12.4MD, 12.4T, 12.4XZ, and 12.4YA allows remote attackers to cause a denial of service (device reload) via a crafted NTPv4 packet, aka Bug IDs CSCsu24505 and CSCsv75948.	2009-09-28	7.8	CVE-2009-2869 VUPEN SECTRACK CISCO CONFIRM OSVDB
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.2 through 12.4, when the Cisco Unified Border Element feature is enabled, allows remote attackers to cause a denial of service (device reload) via crafted SIP messages, aka Bug ID CSCsx25880.	2009-09-28	7.8	CVE-2009-2870 VUPEN SECTRACK CISCO CONFIRM
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.2 and 12.4, when SSLVPN sessions, SSH sessions, or IKE encrypted nonces are enabled, allows remote attackers to cause a denial of service (device reload) via a crafted encrypted packet, aka Bug ID CSCsq24002.	2009-09-28	7.8	CVE-2009-2871 VUPEN SECTRACK CISCO CONFIRM
cisco -- ios	Cisco IOS 12.0 through 12.4, when IP-based tunnels and the Cisco Express Forwarding feature are enabled, allows remote attackers to cause a denial of service (device reload) via malformed packets, aka Bug ID CSCsx70889.	2009-09-28	7.1	CVE-2009-2873 CISCO CONFIRM CONFIRM
coreftp -- core_ftp	Stack-based buffer overflow in Core FTP 2.1 build 1612 allows user-assisted remote attackers to execute arbitrary code via a long hostname in an FTP server entry in a site backup file. NOTE: some of these details are obtained from third party information.	2009-09-30	9.3	CVE-2009-3484 XF MISC SECUNIA OSVDB
dataspheric -- linkspheric	SQL injection vulnerability in viewListing.php in linkSpheric 0.74 Beta 6 allows remote attackers to execute arbitrary SQL commands via the listID parameter.	2009-10-01	7.5	CVE-2009-3510 MILWORM
fastballproductions -- com_fastball	SQL injection vulnerability in the Fastball (com_fastball) component 1.1.0 through 1.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the league parameter to index.php.	2009-09-28	7.5	CVE-2009-3443 SECUNIA MISC
	Multiple PHP remote file inclusion			

fh54 -- justvisual	vulnerabilities in justVisual 1.2 allow remote attackers to execute arbitrary PHP code via a URL in the fs_jVroot parameter to (1) sites/site/pages/index.php, (2) sites/test/pages/contact.php, (3) system/pageTemplate.php, and (4) system/utilities.php.	2009-10-01	7.5	CVE-2009-3511 MILWoRM
globalscape -- cuteftp	Heap-based buffer overflow in the Create New Site feature in GlobalSCAPE CuteFTP Professional, Home, and Lite 8.3.3 and 8.3.3.0054 allows user-assisted remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a site list containing an entry with a long label.	2009-09-30	9.3	CVE-2009-3483 XF MISC OSVDB SECUNIA
google -- chrome	Google Chrome, possibly 3.0.195.21 and earlier, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-29	7.5	CVE-2009-3456 BID
gotdns -- loggix_project	Multiple PHP remote file inclusion vulnerabilities in Loggix Project 9.4.5 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the pathToIndex parameter to (1) Calendar.php, (2) Comment.php, (3) Rss.php and (4) Trackback.php in lib/Loggix/Module/; and (5) modules/downloads/lib/LM_Downloads.php.	2009-09-30	7.5	CVE-2009-3492 XF MILWoRM
hp -- remote_graphics_software	Unspecified vulnerability in the Sender module in HP Remote Graphics Software (RGS) 5.1.3 through 5.2.6 allows remote authenticated users to execute arbitrary code via unknown vectors.	2009-09-29	7.1	CVE-2009-2683 HP HP
ibm -- db2	IBM DB2 8 before FP18, 9.1 before FP8, and 9.5 before FP4 does not perform the expected drops of certain table functions upon a loss of privileges by the functions' definers, which has unspecified impact and remote attack vectors.	2009-09-29	7.5	CVE-2009-3471 BID CONFIRM CONFIRM SECUNIA
ibm -- db2	IBM DB2 9.1 before FP8 does not require the SETSESSIONUSER privilege for the SET SESSION AUTHORIZATION statement, which has unspecified impact and remote attack vectors.	2009-09-29	10.0	CVE-2009-3473 BID CONFIRM AIXAPAR SECUNIA
ibm -- aix	gssd in IBM AIX 5.3.x through 5.3.9 and 6.1.0 through 6.1.2 does not properly handle the NFSv4 Kerberos credential cache, which allows local users to bypass intended access restrictions for Kerberized NFSv4 shares via unspecified vectors.	2009-10-01	7.2	CVE-2009-3516 BID CONFIRM

ibm -- aix	nfs.ext in IBM AIX 5.3.x through 5.3.9 and 6.1.0 through 6.1.2 does not properly use the nfs_portmon setting, which allows remote attackers to bypass intended access restrictions for NFSv4 shares via unspecified vectors.	2009-10-01	10.0	CVE-2009-3517 BID CONFIRM
ibm -- installation_manager	Argument injection vulnerability in the iim: URI handler in IBMIM.exe in IBM Installation Manager 1.3.2 and earlier, as used in IBM Rational Robot and Rational Team Concert, allows remote attackers to load arbitrary DLL files via the -vm option, as demonstrated by a reference to a UNC share pathname.	2009-10-01	9.3	CVE-2009-3518 VUPEN SECUNIA MISC
internet2 -- opensaml internet2 -- shibboleth-sp internet2 -- xmltooling	OpenSAML 2.x before 2.2.1 and XMLTooling 1.x before 1.2.1, as used by Internet2 Shibboleth Service Provider 2.x before 2.2.1, do not follow the KeyDescriptor element's Use attribute, which allows remote attackers to use a certificate for both signing and encryption when it is designated for just one purpose, potentially weakening the intended security application of the certificate.	2009-09-29	7.5	CVE-2009-3474 BID DEBIAN DEBIAN CONFIRM
internet2 -- shibboleth-sp	Internet2 Shibboleth Service Provider software 1.3.x before 1.3.3 and 2.x before 2.2.1, when using PKIX trust validation, does not properly handle a '\o' character in the subject or subjectAltName fields of a certificate, which allows remote man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-29	7.5	CVE-2009-3475 DEBIAN DEBIAN CONFIRM SECUNIA SECUNIA SECUNIA
internet2 -- opensaml internet2 -- shibboleth-sp internet2 -- xmltooling	Buffer overflow in OpenSAML before 1.1.3 as used in Internet2 Shibboleth Service Provider software 1.3.x before 1.3.4, and XMLTooling before 1.2.2 as used in Internet2 Shibboleth Service Provider software 2.x before 2.2.1, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a malformed encoded URL.	2009-09-29	9.3	CVE-2009-3476 XF BID CONFIRM SECUNIA SECUNIA
isxygen -- icrm_basic	SQL injection vulnerability in the iCRM Basic (com_icrbasic) component 1.4.2.31 for Joomla! allows remote attackers to execute arbitrary SQL commands via the p3 parameter to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-30	7.5	CVE-2009-3480 XF BID SECUNIA OSVDB
isxygen -- com_icrbasic	A certain interface in the iCRM Basic (com_icrbasic) component 1.4.2.31 for Joomla! does not require administrative authentication, which has unspecified impact and remote attack vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-30	7.5	CVE-2009-3481 BID OSVDB SECUNIA

jean-michel_wyttenbach -- cmsphp	Directory traversal vulnerability in modules.php in CMSphp 0.21 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the mod_file parameter.	2009-10-01	7.5	CVE-2009-3507 MILWORM SECUNIA
kinfusion -- com_sportfusion	SQL injection vulnerability in the Kinfusion SportFusion (com_sportfusion) component 0.2.2 through 0.2.3 for Joomla! allows remote attackers to execute arbitrary SQL commands via the cid[o] parameter in a teamdetail action to index.php.	2009-09-30	7.5	CVE-2009-3491 BID SECUNIA MISC
maxwebportal -- maxwebportal	Multiple SQL injection vulnerabilities in forum.asp in MaxWebPortal allow remote attackers to execute arbitrary SQL commands via the (1) FORUM_ID or (2) CAT_ID parameter. NOTE: this might overlap CVE-2005-1417.	2009-09-28	7.5	CVE-2009-3436 XF BID MISC
onestopjoomla -- com_tupinambis	SQL injection vulnerability in the Tupinambis (com_tupinambis) component 1.0 for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the proyecto parameter in a verproyecto action to index.php.	2009-09-28	7.5	CVE-2009-3434 XF VUPEN BID SECUNIA MISC
rick_estrada -- com_mytube	SQL injection vulnerability in the MyRemote Video Gallery (com_mytube) component 1.0 Beta for Joomla! allows remote attackers to execute arbitrary SQL commands via the user_id parameter in a videos action to index.php.	2009-09-28	7.5	CVE-2009-3446 XF BID MILWORM
sun -- cluster	Unspecified vulnerability in csetup in the configuration utility in Sun Solaris Cluster 3.2 allows local users to gain privileges via unknown vectors.	2009-09-28	7.2	CVE-2009-3433 SUNALERT
vastal -- dvd_zone	SQL injection vulnerability in view_mag.php in Vastal I-Tech DVD Zone allows remote attackers to execute arbitrary SQL commands via the mag_id parameter, a different vector than CVE-2008-4465.	2009-09-30	7.5	CVE-2009-3495 VUPEN BID SECUNIA MISC
vastal -- agent_zone	SQL injection vulnerability in view_listing.php in Vastal I-Tech Agent Zone (aka The Real Estate Script) allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-09-30	7.5	CVE-2009-3497 MISC SECUNIA
vastal -- mmorpg_zone	SQL injection vulnerability in view_news.php in Vastal I-Tech MMORPG Zone allows remote attackers to execute arbitrary SQL commands via the news_id parameter. NOTE: the game_id vector is already covered by CVE-2008-4460.	2009-09-30	7.5	CVE-2009-3505 XF VUPEN BID MISC
witchakorn_kamolpornwijit -- com_facebook	SQL injection vulnerability in the JoomlaFacebook (com_facebook) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a student action to index.php.	2009-09-28	7.5	CVE-2009-3438 XF VUPEN BID MISC

[Back to top](#)

Medium Vulnerabilities			
Primary Vendor -- Product	Description	Published	CVSS Score
adobe -- photoshop_elements	Adobe Photoshop Elements 8.0 installs the Adobe Active File Monitor V8 service with an insecure security descriptor, which allows local users to (1) stop the service via the stop command, (2) execute arbitrary commands as SYSTEM by using the config command to modify the binPath variable, or (3) restart the service via the start command.	2009-09-30	6.9
alienvault -- ossim	Multiple SQL injection vulnerabilities in Open Source Security Information Management (OSSIM) before 2.1.2 allow remote authenticated users to execute arbitrary SQL commands via the id_document parameter to (1) repository_document.php, (2) repository_links.php, and (3) repository_editdocument.php in repository/; the (4) group parameter to policy/getpolicy.php; the name parameter to (5) host/newhostgroupform.php and (6) net/modifynetform.php; and unspecified other vectors related to the policy menu.	2009-09-28	6.5
alienvault -- ossim	Cross-site scripting (XSS) vulnerability in Open Source Security Information Management (OSSIM) before 2.1.2 allows remote attackers to inject arbitrary web script or HTML via the option parameter to the default URI (aka the main menu).	2009-09-28	4.3
alienvault -- ossim	Open Source Security Information Management (OSSIM) before 2.1.2 allows remote attackers to bypass authentication, and read graphs or infrastructure information, via a direct request to (1) graphs/alarms_events.php or (2) host/draw_tree.php.	2009-09-28	5.0
ariel_barreiro -- meta_tags	The Meta tags (aka Nodewords) module before 6.x-1.1 for Drupal does not properly follow permissions during assignment of node meta tags, which allows remote attackers to obtain sensitive information via unspecified vectors.	2009-09-28	5.0
avast -- avast_antivirus_home avast -- avast_antivirus_professional	aavmKer4.sys in avast! Home and Professional for Windows before 4.8.1356 does not properly validate input to IOCTLs (1) 0xb2d6000c and (2) 0xb2d60034, which allows local users to gain privileges via IOCTL requests using crafted kernel addresses that trigger memory corruption, a different vulnerability than CVE-2008-1625.	2009-10-01	6.9
bakbone -- netvault	npvmgr.exe in BakBone NetVault Backup 8.22 Build 29 allows remote attackers to cause a denial of service (daemon crash) via a packet to (1) TCP or (2) UDP port 20031 with a large value in an unspecified size field, which is not	2009-09-29	5.0

	properly handled in a malloc operation. NOTE: some of these details are obtained from third party information.		
cisco -- ios	The Object Groups for Access Control Lists (ACLs) feature in Cisco IOS 12.2XNB, 12.2XNC, 12.2XND, 12.4MD, 12.4T, 12.4XZ, and 12.4YA allows remote attackers to bypass intended access restrictions via crafted requests, aka Bug IDs CSCsx07114, CSCsu70214, CSCsw47076, CSCsv48603, CSCsy54122, and CSCsu50252.	2009-09-28	4.3
cisco -- ios	Cisco IOS 12.0 through 12.4, when IP-based tunnels and the Cisco Express Forwarding feature are enabled, allows remote attackers to cause a denial of service (device reload) via a malformed packet that is not properly handled during switching from one tunnel to a second tunnel, aka Bug IDs CSCsh97579 and CSCsq31776.	2009-09-28	6.8
cisco -- ace_web_application_firewall cisco -- ace_xml_gateway	Cisco ACE XML Gateway (AXG) and ACE Web Application Firewall (WAF) before 6.1 allow remote attackers to obtain sensitive information via an HTTP request that lacks a handler, as demonstrated by (1) an OPTIONS request or (2) a crafted GET request, leading to a Message-handling Errors message containing a certain client intranet IP address, aka Bug ID CSCtb82159.	2009-09-29	5.0
cj-design -- cj_dynamic_poll	Cross-site scripting (XSS) vulnerability in admin/admin_index.php in CJ Dynamic Poll PRO 2.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-10-01	4.3
code-crafters -- ability_mail_server	Unspecified vulnerability in Code-Crafters Ability Mail Server before 2.70 allows remote attackers to cause a denial of service (daemon crash) via an IMAP4 FETCH command.	2009-09-28	5.0
collectorz -- mp3_collector	MP3 Collector 2.3 allows remote attackers to cause a denial of service (application crash) via a long URL in a .m3u playlist file.	2009-09-29	4.3
	Multiple PHP remote file inclusion vulnerabilities in MaxCMS 3.11.2ob, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) is_projectPath parameter to includes/InstantSite/inc.is_root.php; GLOBALS[thCMS_root] parameter to (2) classes/class.Tree.php, (3) includes/inc.thcms_admin_mediamanager.php, and (4) modul/mod.rssreader.php; is_path parameter to (5) class.tasklist.php, (6) class.thcms.php, (7) class.thcms_content.php, (8) class.thcms_modul_parent.php, (9) class.thcms_page.php, and (10) class.thescm_user.php in classes/; and (11)		

database -- maxcms	includes/InstantSite/class.Tree.php; and thCMS_root parameter to (12) classes/class.thcms_modul.php; (13) inc.page_edit_tasklist.php, (14) inc.thcms_admin_overview_backup.php, and (15) inc.thcms_edit_content.php in includes/; and (16) class.thems_modul_parent_xml.php, (17) mod.cmstranslator.php, (18) mod.download.php, (19) mod.faq.php, (20) mod.guestbook.php, (21) mod.html.php, (22) mod.menu.php, (23) mod.news.php, (24) mod.newsticker.php, (25) mod.rss.php, (26) mod.search.php, (27) mod.sendtofriend.php, (28) mod.sitemap.php, (29) mod.tagdoc.php, (30) mod.template.php, (31) mod.test.php, (32) mod.text.php, (33) mod.upload.php, and (34) mod.users.php in modul/.	2009-09-25	6.8
drupal -- drupal ron_jerome -- bibliography	Cross-site scripting (XSS) vulnerability in Bibliography (Biblio) 5.x before 5.x-1.17 and 6.x before 6.x-1.6, a module for Drupal, allows remote attackers, with "create content displayed by the Bibliography module" permissions, to inject arbitrary web script or HTML via a title.	2009-09-30	4.3
e107 -- e107	Cross-site scripting (XSS) vulnerability in email.php in e107 0.7.16 and earlier allows remote attackers to inject arbitrary web script or HTML via the HTTP Referer header in a news.1 (aka news to email) action.	2009-09-28	4.3
fcgphilipp -- mujecms	Multiple directory traversal vulnerabilities in MUJE CMS 1.0.4.34 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) _class parameter to admin.php and the (2) url parameter to install/install.php; and allow remote authenticated administrators to read arbitrary files via a .. (dot dot) in the (3) _htmlfile parameter to admin.php.	2009-10-01	6.0
fedorahosted -- newt	Heap-based buffer overflow in textbox.c in newt 0.51.5, 0.51.6, and 0.52.2 allows local users to cause a denial of service (application crash) or possibly execute arbitrary code via a request to display a crafted text dialog box.	2009-09-29	4.6
gnu -- wget wget -- wget	GNU Wget before 1.12 does not properly handle a '\o' character in a domain name in the Common Name field of an X.509 certificate, which allows man-in-the-middle remote attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-30	6.8
hbcm -- hbcm	SQL injection vulnerability in php/update_article_hits.php in HBcm 1.7 allows remote attackers to execute arbitrary SQL commands via the article_id parameter.	2009-09-30	6.8

henriksjokvist -- markdown_preview	Cross-site scripting (XSS) vulnerability in the live preview feature in the Markdown Preview module 6.x for Drupal allows remote attackers to inject arbitrary web script or HTML via "Markdown input."	2009-09-28	4.3
hp -- procurve_identity_driven_manager	Unspecified vulnerability in HP ProCurve Identity Driven Manager (IDM) A.02.x through A.02.03 and A.03.x through A.03.00, on Windows Server 2003 with IAS and Windows Server 2008 with NPS, allows local users to gain privileges via unknown vectors.	2009-09-29	6.8
ibm -- lotus_quickr	Multiple cross-site scripting (XSS) vulnerabilities in IBM Lotus Quickr 8.1.0 services for WebSphere Portal allow remote attackers to inject arbitrary web script or HTML via the filename of a .odt file in a Lotus Quickr place, related to the Library template.	2009-09-29	4.3
ibm -- lotus_connections	Cross-site scripting (XSS) vulnerability in profiles/html/simpleSearch.do in IBM Lotus Connections 2.0.1 allows remote attackers to inject arbitrary web script or HTML via the name parameter.	2009-09-29	4.3
ibm -- informix_dynamic_server	IBM Informix Dynamic Server (IDS) 10.00 before 10.00.xC11, 11.10 before 11.10.xC4, and 11.50 before 11.50.xC5 allows remote attackers to cause a denial of service (memory corruption, assertion failure, and daemon crash) by sending a long password over a JDBC connection.	2009-09-29	5.0
ibm -- db2	IBM DB2 8 before FP18, 9.1 before FP8, and 9.5 before FP4 allows remote authenticated users to bypass intended access restrictions, and update, insert, or delete table rows, via unspecified vectors.	2009-09-29	6.5
ibm -- tivoli_composite_application_manager_for_wesbsphere	Multiple cross-site scripting (XSS) vulnerabilities in the Visualization Engine (VE) in IBM Tivoli Composite Application Manager for WebSphere (ITCAM) 6.1.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-10-01	4.3
jean-michel_wyttenbach -- cmsphp	Multiple cross-site scripting (XSS) vulnerabilities in CMSphp 0.21 allow remote attackers to inject arbitrary web script or HTML via the (1) cook_user parameter to index.php and the (2) name parameter to modules.php.	2009-10-01	4.3
jean-michel_wyttenbach -- cmsphp	Cross-site request forgery (CSRF) vulnerability in the Your_account module in CMSphp 0.21 allows remote attackers to hijack the authentication of administrators for requests that change an administrator password via the pseudo, pwd, and uid parameters in an	2009-10-01	6.8

	admin_info_user_verif action.		
juniper -- junos	Cross-site scripting (XSS) vulnerability in the J-Web interface in Juniper JUNOS 8.5R1.14 and 9.0R1.1 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI.	2009-09-30	4.3
marcin_manek -- d.net_cms	Multiple SQL injection vulnerabilities in d.net CMS allow remote attackers to execute arbitrary SQL commands via (1) the page parameter to index.php; and allow remote authenticated administrators to execute arbitrary SQL commands via the (2) edit_id and (3) _p parameter in a news action to dnet_admin/index.php.	2009-10-01	6.5
marcin_manek -- d.net_cms	Directory traversal vulnerability in dnet_admin/index.php in d.net CMS allows remote authenticated administrators to include and execute arbitrary local files via a .. (dot dot) in the type parameter.	2009-10-01	6.5
microsoft -- ie	Microsoft Internet Explorer does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-29	6.8
moshe_weitzman -- devel	Cross-site scripting (XSS) vulnerability in the variable editor in the Devel module 5.x before 5.x-1.2 and 6.x before 6.x-1.18, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via a variable name.	2009-09-28	4.3
nightlight -- fireftp	Argument injection vulnerability in (1) src/content/js/connection/sftp.js and (2) src/content/js/connection/controlSocket.js.in in FireFTP Extension 1.0.5 for Firefox allows remote authenticated SFTP users to cause victims to alter permissions, delete, download, or move the wrong file via a filename containing " (double quotes), which is not properly filtered or encoded when FireFTP constructs the command to send to psftp.exe.	2009-09-29	6.0
openssh -- openssh	A certain Red Hat modification to the ChrootDirectory feature in OpenSSH 4.8, as used in sshd in OpenSSH 4.3 in Red Hat Enterprise Linux (RHEL) 5.4 and Fedora 11, allows local users to gain privileges via hard links to setuid programs that use configuration files within the chroot directory, related to requirements for directory ownership.	2009-10-01	6.9
osisoft -- pi_server	PI Server in OSIsoft PI System before 3.4.380.x does not properly use encryption in the default authentication process, which allows remote attackers to read or modify information in databases via unspecified vectors.	2009-10-01	6.4

phplemon -- myweight	Multiple cross-site scripting (XSS) vulnerabilities in MyWeight 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) date parameter to user_addfood.php, info parameter to (2) user_forgot_pwd_form.php and (3) user_login.php, and (4) return parameter to user_login.php.	2009-10-01	4.3
pilotgroup -- pg_etraining	Multiple cross-site scripting (XSS) vulnerabilities in Pilot Group (PG) eTraining allow remote attackers to inject arbitrary web script or HTML via (1) the cat_id parameter to courses_login.php, the id parameter to (2) news_read.php or (3) lessons_login.php, or (4) the cur parameter in a start action to lessons_login.php.	2009-10-01	4.3
radactive -- i-load	Unrestricted file upload vulnerability in RADactive I-Load before 2008.2.5.0 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, and then sending a request for a predictable filename during a short time window.	2009-09-29	6.8
radactive -- i-load	Multiple cross-site scripting (XSS) vulnerabilities in WebCoreModule.ashx in RADactive I-Load before 2008.2.5.0 allow remote attackers to inject arbitrary web script or HTML via parameters with names beginning with __ (underscore underscore) sequences, which are incompatible with an XSS protection mechanism provided by Microsoft ASP.NET.	2009-09-29	4.3
radactive -- i-load	Directory traversal vulnerability in WebCoreModule.ashx in RADactive I-Load before 2008.2.5.0 allows remote attackers to read arbitrary files via unspecified vectors.	2009-09-29	5.0
radactive -- i-load	WebCoreModule.ashx in RADactive I-Load before 2008.2.5.0 allows remote attackers to obtain sensitive information via unspecified requests that trigger responses containing the saved-image folder pathname.	2009-09-29	5.0
rim -- blackberry_device_software	The Blackberry Browser in RIM BlackBerry Device Software 4.5.0 before 4.5.0.173, 4.6.0 before 4.6.0.303, 4.6.1 before 4.6.1.309, 4.7.0 before 4.7.0.179, and 4.7.1 before 4.7.1.57 does not properly handle "hidden" characters including a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows remote man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-29	6.8
	Multiple unspecified vulnerabilities in Common		

sun -- solaris	Desktop Environment (CDE) in Sun Solaris 10, when Trusted Extensions is enabled, allow local users to execute arbitrary commands or bypass the Mandatory Access Control (MAC) policy via unknown vectors, related to a menu typo and the Style Manager.	2009-09-29	6.9
sun -- opensolaris sun -- solaris	Multiple memory leaks in the IP module in the kernel in Sun Solaris 8 through 10, and OpenSolaris before snv_109, allow local users to cause a denial of service (memory consumption) via vectors related to (1) M_DATA, (2) M_PROTO, (3) M_PCPROTO, and (4) M_SIG STREAMS messages.	2009-10-01	4.9
todor_lazarov -- t-htb_manager	Multiple SQL injection vulnerabilities in index.php in T-HTB Manager 0.5, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via (1) the id parameter in a delete_category action, (2) the name parameter in an update_category action, and other vectors.	2009-09-30	6.8
trustport -- antivirus trustport -- pc_security	TrustPort Antivirus before 2.8.0.2266 and PC Security before 2.0.0.1291 use weak permissions (Everyone: Full Control) for files under %PROGRAMFILES%, which allows local users to gain privileges by replacing executables with Trojan horse programs.	2009-09-30	6.8
vastal -- dvd_zone	Cross-site scripting (XSS) vulnerability in view_mag.php in Vastal I-Tech DVD Zone allows remote attackers to inject arbitrary web script or HTML via the mag_id parameter.	2009-09-30	4.3
zenas -- paobacheca_guestbook	Multiple cross-site scripting (XSS) vulnerabilities in Zenas PaoBacheca Guestbook 2.1 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) scrivi.php and (2) index.php.	2009-09-30	4.3

[Back to top](#)

Low Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
juniper -- junos	Multiple cross-site scripting (XSS) vulnerabilities in the J-Web interface in Juniper JUNOS 8.5R1.14 allow remote authenticated users to inject arbitrary web script or HTML via the host parameter to (1) the pinghost program, reachable through the diagnose program; or (2) the traceroute program, reachable through the diagnose program; or (3) the probe-limit parameter to the configuration program; the (4) wizard-ids or (5) pager-new-identifier parameter in a firewall-filters action to the configuration program; (6) the cos-physical-interface-name parameter in a cos-physical-interfaces-edit action to the configuration program; the (7) wizard-args or (8) wizard-ids parameter in an snmp action to the configuration	2009-09-30	3.5	CVE-2009-3486 VUPEN BID MISC SECUNIA	

	program; the (9) username or (10) fullname parameter in a users action to the configuration program; or the (11) certname or (12) certbody parameter in a local-cert (aka https) action to the configuration program.			
juniper -- junos	Multiple cross-site scripting (XSS) vulnerabilities in the J-Web interface in Juniper JUNOS 8.5R1.14 allow remote authenticated users to inject arbitrary web script or HTML via (1) the JEXEC_OUTID parameter in a JEXEC_MODE_RELAY_OUTPUT action to the jexec program; the (2) act, (3) refresh-time, or (4) ifid parameter to scripter.php; (5) the revision parameter in a rollback action to the configuration program; the m[] parameter to the (6) monitor, (7) manage, (8) events, (9) configuration, or (10) alarms program; (11) the m[] parameter to the default URI; (12) the m[] parameter in a browse action to the default URI; (13) the wizard-next parameter in an https action to the configuration program; or the (14) Contact Information, (15) System Description, (16) Local Engine ID, (17) System Location, or (18) System Name Override SNMP parameter, related to the configuration program.	2009-09-30	3.5	CVE-2009-3487 VUPEN BID MISC SECUNIA
ron_jerome -- bibliography	Cross-site scripting (XSS) vulnerability in the Bibliography (aka Biblio) module 6.x-1.6 for Drupal allows remote authenticated users, with certain content-creation privileges, to inject arbitrary web script or HTML via the Title field, probably a different vulnerability than CVE-2009-3479.	2009-09-30	2.1	CVE-2009-3488 XF BID SECUNIA FULLDISC
sun -- opensolaris sun -- solaris	Unspecified vulnerability in xscreensaver in Sun Solaris 10, and OpenSolaris before snv_112, when Xorg or Xnewt is used and RandR is enabled, allows physically proximate attackers to read a locked screen via unknown vectors related to XRandR resize events.	2009-09-28	1.9	CVE-2009-3432 BID SUNALERT CONFIRM

[Back to top](#)

Last updated October 05, 2009

 Print This Document